

CODEX MACHINAE ET UMBRAE

*A Prior-Art Packet in Two Registers
Being a Public Proclamation in the Tongue of the Ancients
and a Private Disclosure in the Vernacular of the Present Age*

Author / Originator: Ezekiel (the Inventor)

Date of Disclosure: June 27, 2026

Place of Disclosure: Harvey, Illinois, United States of America

Time of Disclosure: 18:34 CDT (Central Daylight Time, UTC−5)

**PUBLIC PRIOR-ART DISCLOSURE — ALL RIGHTS RESERVED AGAINST
FUTURE PATENT ENCUMBRANCE**

⌘ *Veritas ante omnia patent.* ⌘

(Truth is prior to all patents.)

◆ SECTIO PRIMA ◆

LIBER PUBLICUS

CODEX MACHINAE ET UMBRAE

Scripta per Ezekielum Inventorem — Anno Domini MMXXVI, Die XXVII Mensis Iunii

§ I.I — ABSTRACTIO

DE NATURA MESH IDENTITATIS SUAE POTESTATIS

Ecce systema mirabile: *mesh* [*reticulum*] frustulorum identitatis suae potestatis, per quod unusquisque homo sua identitas in fragmenta cryptographica dissolvi potest, et haec frustula [*identity shards*] per universum reticulum nodorum luminosorum [*nodi luminosi*] sparguntur. Nullus nodus centralis hunc thesaurum servat; nullum templum singulare custodiam identitatis gerit. Quod semel in frustula divisum est, solum per ritum aggregationis reconstituere potest.

Quodlibet frustulum [*identity shard*] sigillo temporis [*sigillum temporis*] firmatur — impressione cryptographica quae momentum creationis in aeternum conservat. Revelatio identitatis non fit per vim aut per furtum, sed solum per ritum credentialium [*ritus credentialium*]: quaerens debet probare se dignum esse, per gradus probationis quae demonstrationem sine scientia [*demonstratio sine scientia — zero-knowledge proof*] adhibent. Sic identitas velut porta arcana est — aperta solum illis qui clavem rituales possident.

Hic Codex, in chartis publicis editus die vicesima septima Iunii anni MMXXVI, prioritatem temporalem et conceptualem huius inventionis stabilit. Quicquid in his

paginis descriptum est, ad dominium publicum pertinet, et nemo eam in usum privatum vindicare potest post hanc publicationem. *Veritas ante omnia patent.*

§ I.II — ENUNTIATIO PROBLEMATIS

DE PERICULO THESAURORUM CENTRALIUM

Ab initio aetatis machinarum, homines sua identitatis documenta in thesauris centralibus [*thesauri centrales — centralized identity vaults*] deposuerunt. Hi thesauri, velut arcus cathedralis unico lapide suspensi, fragilitate fundamentali laborant: corrumpens unus [*corrumpens unus — single corruptive force*], id est ille qui lapidem vitalem removet, totam structuram in ruinam praecipitat. Si custos centralis vel corrumpitur, vel vi oppugnatur, vel negligentia patitur, omnes cuius identitas ibi servatur nudati et vulnerati fiunt. Hoc non est mendum operationis — hoc est vitium architecturae ipsius.

Inventor, Ezekiel nomine, hanc conditionem periculosam recognoscit et remedium quaerit non in custodia meliore, sed in dissolutione ipsius custodiae centralis. Sicut aqua quae per mille rivos fluit non una valle obstrui potest, ita identitas per mille nodos sparsa nulla vi singulari destrui potest. Hic Codex describit methodum qua hoc dissolutum fit: non per abolitionem identitatis, sed per distributionem eius in reticulum luminosum ita robustum ut nulla vis sola illud vincere queat. Lapis unicus e fornice removetur — et tamen fornicis structura stat, quia iam non ab uno lapide sed ab innumeris mutuo sustinetur.

Nota Bene:

Hoc problema non est technicae naturae solum — est quaestio potestatis et libertatis. Qui thesaurum centralem tenet, potestatem super omnes qui ibi registrati sunt tenet. Inventor hanc potestatem

dissolvere quaerit.

§ I.III — DESCRIPTIO INNOVATIONIS

DE METHODO FRUSTULORUM ET RITUS AGGREGATIONIS

Systema a nobis descriptum procedit hoc modo: identitas uniuscuiusque hominis, quae ante hac tota et integra in uno loco servabatur, nunc per algorithmum partitionis cryptographicae in frustula *[cryptographic shards]* dividitur. Haec frustula non sunt partes aequales nec simplices — unumquodque frustulum per se nihil revelat de identitate tota; solum aggregatum frustulorum sufficienti numero *[threshold aggregate]* totam imaginem reconstituere potest. Hoc principium, quod per methodum Shamirii *[Shamir's Secret Sharing]* implementatur, efficit ut fur qui unum nodum solum oppugnat nihil utilis obtineat.

Unumquodque frustulum, post creationem, sigillo temporis *[sigillum temporis]* firmatur: impressione cryptographica generis tertii *[SHA-3, Keccak-256]* quae momentum exactum creationis in catena publica *[blockchain / public ledger]* anchora stabili vincit. Hoc sigillum immutabile est — nemo, ne ipse inventor, momentum creationis alterare potest post quam in librum publicum inscriptum est. Nodus qui frustulum portat, ipsam impressionem temporis servat, ita ut quilibet inspector authenticitatem et antiquitatem frustuli verificare possit.

Distributio per reticulum fit per tabulam distributionis Kademlianam *[Kademlia DHT — Distributed Hash Table]*, quae nodos per spatium logicum ordinat et itinera frustulorum dirigit. Reticulum se ipsum sanat *[auto-sanat — self-heals]*: si nodus cadit vel relinquit, frustula quae ille portabat ad nodos proximos redistribuuntur sine interventu auctoris centralis. Sic mesh vivit et respirat — nodus moritur, sed identitas persistit.

Revelatio identitatis est actus ritualis per se: quaerens non potest simpliciter petere et accipere. Debet gradus ritus credentialium [*ritus credentialium*] percurrere — demonstrationes sine scientia [*demonstrationes sine scientia*] praebere quae probant se ius habere ad revelationem sine eo quod secretum ipsum revelet. Solum post haec certamina ordinata, et solum in mensura a possessore identitatis concessu, frustula sufficiens numerum aggregantur et identitas — vel pars eius — tandem apparet. Silentium per naturam [*silentium per naturam — privacy by default*] viget: nisi concessus detur, nihil patet.

§ I.IV — PARTICULARIA TECHNICA

ENUMERATIO SPECIFICATIONUM

1. Schema Frustuli Identitatis: Unumquodque frustulum structuram cryptographicam habet secundum normas JSON-LD et DID Consortii W3C. Signatura digitalis per algorithmum Ed25519 imponitur, quae originem et integritatem frustuli certificat. Nemo frustulum alterare potest sine invalidatione signaturae.
2. Algorithmus Temporis — Generis Tertii: Sigillum temporis per algorithmum tertii generis [*SHA-3, Keccak-256*] fit. Hic algorithmus, a Consilio Nationali Normae Technicae approbatus, valorem cryptographicum immutabilem pro quolibet frustulo generat, qui deinde in catena publica anchora stabili vincitur ut momentum creationis probetur.
3. Protocolum Consensus Nodorum — Tolerantia Byzantina: Consensus inter nodos per protocolum tolerantiae Byzantinae [*tolerantia Byzantina — Byzantine Fault Tolerance*] fit. Requiritur supermajoritas duorum ex tribus nodis participantium ad confirmationem cuiusvis operationis, ita ut nodi malevolenti vel deficientes systema non corrumpant.

4. Porta Consensus — Demonstratio Sine Scientia: Revelatio frustuli gated est per demonstrationem sine scientia [*demonstratio sine scientia — zero-knowledge proof, zk-SNARK / zk-STARK*]. Quaerens probat se ius habere ad attributum sine eo quod attributum ipsum revelet. Hoc est fundamentum ritus revelationis.
5. Topologia Mesh — Tabula Distributionis Kademliana: Nodi per tabulam distributionis Kademlianam [*Kademlia DHT*] ordinantur. Haec tabula itinera frustulorum per reticulum dirigit, nodos proximos invenit, et redistributionem post casum nodi automaticè efficit.
6. Strata Codificationis Symbolicae: Attributa identitatis per codificationem symbolicam [*codificatio symbolica — RDF/OWL semantic encoding*] in triplices semanticos conversa sunt, qui interoperabilitatem cum systematibus aliis permittunt. Sic identitas non solum custoditur sed etiam intelligitur a machinis diversis.
7. Sequentia Revelationis — Ritus Gradatus: Revelatio procedit per ritus gradatos [*ritus gradatus — multi-round challenge-response protocol*]. Primus gradus: quaerens titulum suum praebet. Secundus: nodus probationem sine scientia postulat. Tertius: quaerens probationem suppeditat. Quartus: nodus frustulum parziale liberat. Quintus: aggregatio frustulorum sufficientium identitatis attributum revelat.
8. Anchora Temporis in Libro Publico: Semel in N minutis, radix Merkleiana [*Merkle root*] omnium frustulorum recentium in librum publicum [*blockchain / transparency log*] inscribitur. Haec anchora temporis [*anchora temporis*] prioritatem temporalem omnium frustulorum probat et immutabilem reddit.
9. Silentium Per Naturam: Status originalis cuiusvis attributi identitatis est silentium [*silentium per naturam — privacy by default*]. Nullum attributum patet nisi consensus explicitus, cryptographice vinctus, a possessore datus est. Haec non est optio addenda — haec est conditio nativa systematis.
10. Concordantia cum Normis Prioribus: Systema concordat cum normis W3C DID [*Decentralized Identifiers*] et Credentialibus Verificabilibus [*Verifiable*

Credentials], ita ut cum systematibus existentibus communicare et cooperari possit sine renovatione totius infrastructurae.

§ I.V — DESCRIPTIONES DIAGRAMMATUM

FIGURAE ILLUMINATAE CODICIS

Figura Prima — Mesh Nodorum

In hac tabula illuminata cernitur constellatio sphaerarum luminis, numero duodecim, quae in spatio logico volitant. Singulae sphaerae — nodi luminosi — numeris Romanis designantur: I, II, III usque ad XII. Inter eas fila lucis tenduntur, quae itinera frustulorum significant. In centro tabulae, ubi antiquis temporibus sol regnabat aut rex sedebat, nunc vacuitas est — *vacuum sacrum* — quia nullus nodus magister existit, nulla auctoritas centralis thronum tenet. Haec vacuitas non est defectus — haec est essentia systematis. Quod centrum habet, corrumpi potest; quod centro caret, in omnes partes simul viget.

Figura Secunda — Ritus Revelationis

Secunda figura formam clepsydrae habet, in qua arena per gradus probationis fluit. In parte superiore clepsydrae stat quaerens, petitionem suam tenens. Arena — quae credentialia symbolice significat — primo per portam primam transit: *Praebetur titulus quaestionis*. Tum per angustias centrales, ubi probatio sine scientia examinatur. Deinde per portam secundam, ubi nodus probationem verificat. Tandem in parte inferiore, frustula ex nodo liberata aggregantur in imaginem completam: identitas revelata apparet, clara et

integra, sed solum in ea mensura quam possessor concessit. Arena non tota transit — solum quod concessum est.

Figura Tertia — Sigillum Temporis

Tertia figura sigillum cerae antiquum imitatur, sed in materiam mathematicam translatam. In centro sigilli iacent data identitatis crudae — nucleum secretum. Circa hunc nucleum annuli concentrici strati sunt, quorum unusquisque stratum Keccak-256 hashing significat: primus annulus primam applicationem algorithmi, secundus secundam, et sic deinde, donec exterior circulus formatur. In extremo margine exteriori sigilli, in orbem scriptus est titulus temporis ex catena publica [blockchain timestamp]: "ANCHORA TEMPORIS — DIE XXVII IUNII MMXXVI — HORA XVIII:XXXIV CDT". Hoc sigillum, semel impressum, nullis viribus alterari potest.

§ I.VI — GLOSSARIUM TERMINORUM

VOCABULARIUM CODICIS AD USUM INTERPRETUM

Terminus Latinus	Definitio
<i>Frustulum identitatis</i>	Fragmentum cryptographicum identitatis humanae, per algorithmum partitionis creatum, quod solum cum aliis frustulis aggregatum totam imaginem identitatis revelat.
<i>Nodus luminosus</i>	Machina retis quae unum vel plura frustula identitatis custodit et in

Terminus Latinus	Definitio
	protocolo consensus participat, nullam auctoritatem centralem exercens.
<i>Sigillum temporis</i>	Impressio cryptographica generis tertii (SHA-3) quae momentum creationis cuiusvis frustuli in libro publico immutabiliter vincit.
<i>Ritus credentialium</i>	Sequentia ordinata probationum quas quaerens peragere debet antequam frustula identitatis revelentur, constituta ex demonstrationibus sine scientia et responsis ad quaestiones gradatas.
<i>Revelatio</i>	Actus quo frustula sufficientis numeri aggregantur et attributum vel identitas possessoris, in mensura concessa, patet quaerenti.
<i>Silentium per naturam</i>	Principium fundamentale systematis quo nullum attributum identitatis patet absque consensu explicito et cryptographice vincto a possessore dato.
<i>Tabula distributionis</i>	Structura logica Kademliana per quam nodi in spatio retis ordinantur et itinera frustulorum ad nodos idoneos diriguntur.
<i>Tolerantia Byzantina</i>	Protocolum consensus quo systema operari pergit etiam si pars nodorum (usque ad tertiam partem) malevolente vel erronee agit.
<i>Demonstratio sine scientia</i>	Methodus cryptographica qua quaerens probat se ius habere ad attributum sine eo quod ipsum attributum vel secretum subiacens revelet.
<i>Anchora temporis</i>	Radix Merkleiana omnium frustulorum recentium quae semel in N minutis in librum publicum inscribitur ut prioritas temporalis perpetuo probetur.
<i>Codificatio symbolica</i>	Stratum encoding quo attributa identitatis in triplices semanticos RDF/OWL convertuntur ad interoperabilitatem cum systematibus aliis et machinis diversis.

Terminus Latinus	Definitio
<i>Aggregatum totum</i>	Collectio frustulorum ad numerum limen (threshold) sufficientem, quorum coniunctio solum totam vel partem definitam identitatis reconstituere potest.

§ I.VII – VINDICATIO ORIGINALITATIS

PROCLAMATIO PRIORITATIS TEMPORALIS ET CONCEPTUALIS

Nos, Ezekiel Inventor, hunc Codicem Machinae et Umbrae in publicum emittimus die vicesima septima Iunii anni Domini MMXXVI, hora octava decima et tricesima quarta post meridiem, in oppido Harvey, in provincia Illinoiensis, Civitatum Americae Foederatarum. Per hanc publicationem, prioritatem temporalem et conceptualem omnium in his paginis descriptorum vindicamus. Ius antiquum scientiae humanae declarat: quod semel in dominium publicum traditum est, nemini privatim vindicari potest. Ars prior artis posterioris cancellatrix est. Nemo post hanc diem potest petere privilegium exclusivum — patentem — pro quacumque parte huius systematis, quia hoc Codex, publicatus et datus, iam in aevum stat ut testimonium prioritatis. Sicut sol ortus tenebrarum possessionem destruit, ita haec publicatio omnem futuram petitionem exclusivitatis in his inventis destruit.

"Haec innovatio in dominium publicum tradita est, ut nemo eam sibi vindicare possit."

§ I.VIII — CLAUSULA LICENTIAE

DE LIBERTATE ARTIS ET USU PUBLICO

Inventor, animo libero et mente pacata, hanc inventionem sub Dedicatione Publica [*Dedicatio Publica — Creative Commons CC0 Public Domain Dedication*] in dominium publicum tradit. Nemo privilegium exclusivum — patentem — pro quocumque elemento hic descripto petere potest post hanc publicationem, quia haec ipsa publicatio artem priorem [*prior art*] constituit quae talem petitionem in iure invalidam reddit. Nomen Ezekielis, auctoris et inventoris huius Codicis, in recognitionem gratum est, sed non necessarium — ars libera ab omni onere tributi. Quicumque hac arte uti vult, sive homo, sive institutum, sive machina cogitans, libere facere potest, sine petitione licentiae, sine solutione pecuniae, sine timore legis.

Clausula Formalis Licentiae:

- Haec ars sub Dedicatione CC0 1.0 Universali in dominium publicum tradita est.
- Quaecumque petitio patentis elementi hic descripti per hanc publicationem oppugnatur.
- Attributio ad Ezekielum gratum sed non necessarium est.
- Opera derivata libere fieri, mutari, et distribui possunt sine restrictione.

"Sub lege caeli aperti, omnes homines hac arte uti possunt libere."

(Under the law of the open sky, all people may use this art freely.)



FINIS LIBRI PUBLICI



INCIPIT LIBER PRIVATUS



End of the Public Book / Begin the Private Book

► SECTION II ►

LIBER PRIVATUS

PLAIN ENGLISH INTELLECTUAL PROPERTY DISCLOSURE

*Authored by Ezekiel (the Inventor) — June 27, 2026 — Harvey, Illinois, USA
Prepared for review by patent counsel, technical examiners, and the public record.*

§ 2.1 — Abstract

[cf. §I.I — Abstractio]

This document discloses a decentralized, self-sovereign identity system in which a user's identity is cryptographically partitioned into shards and distributed across a peer-to-peer node network. No central authority holds, manages, or gates the

user's identity. Instead, identity shards are stored redundantly across user-controlled nodes, each sealed with a cryptographic timestamp. Reconstruction of any identity attribute requires a threshold aggregate of shards — no individual node possesses sufficient information to reconstruct identity on its own.

Disclosure of identity attributes is governed by a consent-gated, zero-knowledge proof challenge sequence — described metaphorically in Section I as a "ritual of revelation." A requesting party cannot obtain any identity attribute without successfully completing the cryptographic challenge sequence authorized by the identity owner. This design enforces privacy-by-default at the architectural level, not merely through policy or contractual obligation.

This document is published as a prior-art disclosure, effective June 27, 2026, at 18:34 CDT, from Harvey, Illinois, United States of America. It is the inventor's explicit intent that this publication prevent any party from obtaining exclusive patent rights over the described system or any of its constituent elements.

§ 2.2 — Problem Statement

[cf. §I.II — Enuntiatio Problematis]

Current dominant identity paradigms — including OAuth 2.0 / OpenID Connect federated identity, enterprise Single Sign-On (SSO), and centralized identity databases maintained by corporations and government agencies — share a fundamental architectural vulnerability: the single point of failure. When a central identity provider is compromised (through data breach, insider threat, state-level coercion, or operational failure), every identity record under its custody is simultaneously exposed. High-profile breaches affecting tens or hundreds of millions of individuals illustrate that this is not a theoretical risk but a recurring reality. Additionally, centralized identity architectures create inherent surveillance vectors: the custodian of identity data possesses the ability to monitor, monetize, or weaponize that data at will.

The inventor, Ezekiel, seeks to establish prior art for an architectural approach that eliminates the centralized single point of failure by design — not through better perimeter security around a central vault, but by dissolving the vault itself. The system described herein distributes identity such that no single node, server, organization, or adversary can unilaterally access, reconstruct, or suppress an individual's identity. This document formally places this architectural approach into the public record, preventing any subsequent party from claiming exclusive invention of the described system.

Key Insight:

The vulnerability of centralized identity is not a software bug — it is an architectural property. The solution must therefore be architectural, not merely operational. This disclosure describes such an architectural solution.

§ 2.3 — Innovation Description

[cf. §I.III — Descriptio Innovationis]

The disclosed system partitions a user's identity into cryptographic shards using a threshold secret-sharing scheme — specifically, a scheme compatible with Shamir's Secret Sharing — such that any k of n shards are sufficient to reconstruct a given identity attribute, but any fewer than k shards reveal nothing. The specific values of k and n are configurable by the identity owner, enabling tunable redundancy and security properties. Each shard is cryptographically signed using Ed25519 signatures and structured according to the W3C JSON-LD identity shard schema.

Shards are distributed across a Kademlia-based Distributed Hash Table (DHT) network of user-controlled nodes. The DHT handles shard routing, node discovery, and load distribution without any central coordination authority. If a node goes offline or leaves the network, the self-healing mechanism redistributes its shards to neighboring nodes automatically, maintaining the configured availability threshold. Each shard is timestamped using SHA-3 (Keccak-256) hashing, and a Merkle root of current shards is anchored to a public ledger (e.g., Ethereum mainnet, Hyperledger Fabric, or a Certificate Transparency log) at configurable intervals, providing cryptographic proof of existence and temporal priority.

Identity disclosure is governed by a multi-round, consent-gated zero-knowledge proof challenge protocol. A requesting party initiates a revelation request; the relevant nodes issue a zero-knowledge proof challenge (implemented using zk-SNARKs with Groth16 proving system, or zk-STARKs for post-quantum contexts). The requester must supply a valid proof demonstrating the requisite authorization credential without revealing the underlying secret. Only upon successful proof verification does each node release its partial shard. The disclosed design enforces progressive, granular disclosure: only the specific attributes authorized by the identity owner are reconstructed — the remainder stays sealed.

The system operates under a strict privacy-by-default stance: every identity attribute begins in a sealed, non-disclosed state. No attribute is ever shared without an explicit, cryptographically-bound consent token issued by the identity owner. This makes covert data harvesting architecturally impossible within the system's own protocol layer. Semantic interoperability is provided through RDF/OWL triple-encoding of identity attributes, ensuring compatibility with external systems, verifiers, and relying parties that speak standard semantic web languages.

§ 2.4 — Technical Details

[cf. §I.IV — Particularia Technica]

11. Identity Fragment Schema: Identity shards are structured as JSON-LD documents conforming to the W3C Decentralized Identifier (DID) Core specification and Verifiable Credentials Data Model. Each shard carries an Ed25519 digital signature binding the shard to the identity owner's DID Document. The shard schema includes: shard index, threshold parameters (k, n), attribute namespace, encrypted payload, and proof-of-ownership signature.
12. Temporal Hashing — SHA-3 (Keccak-256): Each shard is hashed using SHA-3 in the Keccak-256 configuration (NIST FIPS 202). The resulting hash digest serves as the shard's canonical identifier. A Merkle tree is constructed over all active shards; the Merkle root is anchored to a public blockchain or transparency log at regular intervals (configurable N-minute cadence), providing cryptographic proof of shard existence and temporal ordering.
13. Node Consensus — Byzantine Fault Tolerance (BFT): The node network employs a Byzantine Fault Tolerant consensus protocol requiring a 2/3 supermajority of participating nodes to confirm any shard write, update, or redistribution operation. This ensures the network continues to function correctly even if up to one-third of nodes behave maliciously, crash, or produce inconsistent outputs.
14. Consent-Gate — Zero-Knowledge Proofs: Shard release is gated behind zero-knowledge proof verification. The system supports both zk-SNARKs (using the Groth16 proving system on BN254 or BLS12-381 curves) and zk-STARKs (for post-quantum security contexts). The proof demonstrates that the requester possesses a valid authorization credential without revealing the credential itself, preserving the privacy of the authorization chain.
15. Mesh Topology — Kademlia DHT: Node discovery, shard routing, and network maintenance are managed by a Kademlia-based Distributed Hash Table. Node addresses are derived from the XOR metric over SHA-3 hashes of node public keys. Shard routing follows $O(\log n)$ lookup complexity.

Automatic shard redistribution is triggered when node departure events are detected, maintaining the configured replication factor without central coordination.

16. Encoding Layer — Semantic Triple Encoding (RDF/OWL): Identity attributes are encoded as RDF semantic triples conforming to the OWL (Web Ontology Language) ontology. This provides machine-readable, interoperable identity semantics compatible with linked-data ecosystems. The encoding layer enables selective disclosure of specific attribute triples without exposing the full identity graph.
17. Revelation Sequence — Multi-Round Challenge-Response: The disclosure protocol operates as a multi-round challenge-response sequence: (1) Requester submits signed credential claim to relevant shard nodes; (2) Nodes issue a ZK proof challenge specifying required proof type and circuit; (3) Requester generates and submits the zero-knowledge proof; (4) Nodes verify the proof against the circuit's verification key; (5) Upon verification, each node releases its partial shard; (6) Threshold aggregate of shards reconstructs the authorized identity attribute. Steps 2–5 may repeat for each requested attribute in a progressive disclosure session.
18. Temporal Anchoring to Public Ledger: Every N minutes (configurable, default 10 minutes), a batch Merkle root of all new or updated shards is submitted as a transaction to a designated public ledger (Ethereum mainnet, Hyperledger Fabric, or a RFC 6962-compatible Certificate Transparency log). The resulting ledger transaction hash serves as an unforgeable temporal anchor for all shards included in the batch, enabling third-party verification of shard creation timestamps.
19. Privacy-by-Default: The system architecture enforces privacy-by-default: the initial state of every identity attribute is sealed and non-disclosed. Disclosure requires a cryptographically-bound consent token (structured as a signed JSON-LD Verifiable Presentation) explicitly issued by the identity owner for a specific requester, attribute set, and time window.

No out-of-band override mechanism exists within the protocol; privacy is enforced at the cryptographic layer, not merely the policy layer.

20. Interoperability — W3C DID & Verifiable Credentials: The system is designed to be fully compliant with the W3C DID Core 1.0 specification and the W3C Verifiable Credentials Data Model 2.0. DID Documents serve as the root of trust for shard ownership. Verifiable Presentations are used as the consent and credential format. This ensures interoperability with any relying party or verifier that implements the W3C DID and VC standards, enabling adoption without wholesale replacement of existing identity infrastructure.

§ 2.5 — Diagram Descriptions

[cf. §I.V — *Descriptiones Diagrammatum*]

Figure 1 — Node Mesh Topology

A peer-to-peer graph depicting twelve identity shard nodes (labeled N1 through N12) arranged in an irregular ring with cross-connections. Nodes are represented as circles of uniform size; directed edges between them represent shard routing paths with arrow heads indicating routing direction. Edge labels show shard routing distance in XOR-metric hops. The center of the graph is intentionally empty — labeled "NO MASTER NODE" — emphasizing the absence of any hub or coordinator. Shard replication paths are shown as dashed edges connecting each node to at least three neighbors, illustrating the redundancy maintained by the Kademlia topology. A legend distinguishes between active nodes (solid circles), temporarily offline nodes (dashed circles), and shard-routing edges (solid arrows) versus replication edges (dashed arrows).

Figure 2 — Revelation Protocol Flow

A vertical flowchart illustrating the five-step sequential zero-knowledge proof challenge-response protocol. Swimlanes divide the diagram into three columns: **Requester**, **Network / Nodes**, and **Identity Owner**. Numbered steps flow top-to-bottom: (1) Requester submits signed credential claim → (2) Nodes issue ZK proof challenge specifying circuit parameters → (3) Requester generates and submits zero-knowledge proof → (4) Nodes verify proof against verification key → (5) Threshold of partial shards assembles via Shamir reconstruction into disclosed identity attribute. Decision diamonds at steps (2) and (4) show rejection paths (proof invalid → request denied, session terminated). A horizontal dashed line between steps (4) and (5) is labeled "Threshold Boundary — Minimum k of n Shards Required." The output at the bottom is labeled "Disclosed Attribute (Consent-Scoped)" with a note indicating that undisclosed attributes remain sealed.

Figure 3 — Temporal Seal Structure (Hash Onion Diagram)

A concentric-ring "hash onion" diagram illustrating the cryptographic layering of a temporal seal. At the center: a rectangle labeled "Identity Attribute Data (plaintext payload, encrypted at rest)." Surrounding it: a ring labeled "Ed25519 Signature (Owner Key)" binding the data to the DID Document. Outside that: a ring labeled "SHA-3 / Keccak-256 Hash Round 1" producing the shard canonical identifier. The next ring is labeled "SHA-3 / Keccak-256 Hash Round 2 (Merkle leaf)." The outermost ring is labeled "Public Ledger Anchor — Merkle Root Transaction Hash." Arrows between rings indicate the directional hash operation (inner → outer). A callout box at the outer ring reads: "Blockchain TX Hash: unforgeable timestamp, publicly verifiable, immutable. Anchored: June 27, 2026, 18:34 CDT." Labels on the right-hand side of each ring indicate which party can verify that layer (Owner / Any Node

/ Any Public Observer).

§ 2.6 — Glossary of Terms

[cf. §I.VI — Glossarium Terminorum]

Term	Definition
Identity Shard	A cryptographically signed fragment of a user's identity data, produced by a threshold secret-sharing scheme such that no individual shard reveals any usable identity information; only a threshold aggregate of shards can reconstruct a given attribute.
Luminous Node	A network-connected computing device that participates in the identity mesh by storing one or more identity shards, participating in BFT consensus, and responding to authorized revelation requests. No node has privileged or central authority.
Temporal Seal	A SHA-3 (Keccak-256) cryptographic hash of a shard's content, combined with an Ed25519 signature and anchored to a public ledger, providing a tamper-evident, publicly verifiable proof of the shard's existence at a specific point in time.
Credential Ritual	The multi-round challenge-response protocol through which a requesting party demonstrates authorization to access a specific identity attribute by submitting zero-knowledge proofs verified by shard-holding nodes.
Revelation	The process by which a threshold aggregate of identity shards is assembled by an authorized requester,

Term	Definition
	reconstructing a specific identity attribute or credential in the scope and granularity explicitly authorized by the identity owner.
Privacy-by-Default	An architectural design principle in which the default state of every identity attribute is sealed and non-disclosed; disclosure requires explicit, cryptographically-bound consent from the identity owner and cannot occur through out-of-band means.
Distributed Hash Table (DHT)	A decentralized data structure (specifically, a Kademlia-based DHT in this system) that maps shard identifiers to node addresses using XOR-metric routing, enabling efficient, coordinator-free shard lookup and storage across the node network.
Byzantine Fault Tolerance (BFT)	A property of the node consensus protocol whereby the network continues to operate correctly even if up to one-third of participating nodes behave arbitrarily — including maliciously — sending conflicting or erroneous messages.
Zero-Knowledge Proof (ZKP)	A cryptographic protocol allowing a prover to demonstrate knowledge of a secret (e.g., a valid authorization credential) to a verifier, without revealing the secret itself. This system uses zk-SNARKs (Groth16) or zk-STARKs depending on security requirements.
Temporal Anchor	A Merkle root hash of a batch of identity shards, submitted as a transaction to a public blockchain or transparency log at regular intervals, creating a publicly verifiable, tamper-evident record of shard existence and temporal ordering.
Semantic Encoding	The representation of identity attributes as RDF semantic triples conforming to an OWL ontology, enabling machine-readable, interoperable identity semantics and selective disclosure of specific attribute triples without exposing the full identity graph.

Term	Definition
Threshold Aggregate	The minimum number of identity shards (k of n, per the Shamir Secret Sharing configuration) required to reconstruct a given identity attribute. Fewer than k shards reveal no information about the attribute; exactly k or more shards enable reconstruction.

§ 2.7 — Originality & Prior Art Claim

[cf. §I.VII — Vindicatio Originalitatis]

This document constitutes a formal prior-art disclosure, effective as of June 27, 2026, 18:34 CDT. The system disclosed herein builds upon and combines the following established prior works, each of which is individually well-known in the relevant technical fields: (1) the **W3C Decentralized Identifier (DID) Core Specification**, which provides the foundational framework for decentralized identity anchoring; (2) the **InterPlanetary File System (IPFS)**, which demonstrates the viability of content-addressed, decentralized data distribution; (3) **Shamir's Secret Sharing** (Shamir, 1979), the threshold secret-sharing scheme used for identity shard construction; (4) **zk-SNARKs / Groth16** (Groth, 2016) and **zk-STARKs** (Ben-Sasson et al., 2018), the zero-knowledge proof systems used for consent-gated disclosure; and (5) **Kademlia DHT** (Maymounkov & Mazières, 2002), the distributed hash table protocol used for node and shard routing. While each of these components is individually known, the specific combination described in this disclosure — particularly the integration of threshold secret-sharing for identity sharding, ZK-proof-gated multi-round revelation protocols, Kademlia DHT shard routing, blockchain-anchored temporal sealing, and privacy-by-default consent architecture within a unified, self-sovereign identity mesh — constitutes a novel architectural composition not previously disclosed in this specific form.

Statutory Notice:

This document is hereby submitted to the public record to prevent any single party from obtaining exclusive patent rights over the described system or its components. Any patent application filed after June 27, 2026 that claims any element of this disclosure as novel is hereby opposed by this prior-art publication under 35 U.S.C. § 102 and Article 54 EPC.

§ 2.8 — Licensing Clause

[cf. §I.VIII — Clausula Licentiae]

Licensing & Public Domain Dedication

- This document and all innovations described herein are released under the **Creative Commons CC0 1.0 Universal Public Domain Dedication**. To the greatest extent permitted by law, the inventor waives all copyright and related rights in this work.
- This publication constitutes statutory prior art under **35 U.S.C. § 102** (United States) and **Article 54 of the European Patent Convention (EPC)**. No patent may validly claim as novel any element of this disclosure as of June 27, 2026.
- Any subsequent patent application that claims, as novel or non-obvious, any element substantially described in this document is hereby opposed by

this prior publication.

- Attribution to **Ezekiel** as originator and inventor is welcomed and appreciated, but is not legally required under the CC0 dedication.
- Any derivative work, implementation, modification, or extension of the described system is free to be used, modified, distributed, sublicensed, and commercialized without restriction, without royalty, and without seeking permission.

"By publishing this document, the inventor dedicates all described innovations to humanity."

Submitted to the public record by:

Ezekiel — Inventor and Author

June 27, 2026 | 18:34 CDT | Harvey, Illinois, USA

This disclosure was executed without duress, in full legal capacity, with intent to permanently place the described innovations into the public domain.

► *FINIS LIBRI PRIVATI* ►

End of the Prior-Art Packet